ALGEBRAIC SYSTEMS
Exam 1
September 25, 2006

The point value of each problem is given in the margin. Total = 80 points.

(8) 1. State and prove the cancellation law for addition of integers.
   If \( a + x = a + y \) then \( x = y \).

   Proof.
   \[
   a + x = a + y \\
   -a + (a + x) = -a + (a + y) \\
   \text{additive inverses exist} \\
   (-a + a) + x = (-a + a) + y \\
   \text{associative law} \\
   0 + x = 0 + y \\
   \text{additive inverse property} \\
   x = y \\
   \text{zero is additive identity}
   \]

(10) 2. Use the Euclidean Algorithm to find the greatest common divisor \( d \) of 65 and 91 and find integers \( x, y \) such that \( 65x + 91y = d \).

\[
gcd(65, 91) = gcd(65, 26) = gcd(13, 26) = gcd(13, 0) = 13
\]

\[
\begin{array}{cccc}
65 & 91 & 26 & 13 \\
26 & 91 & 65 & 13 \\
26 & 26 & 13 & 0 \\
0 & 26 & 13 & -1 \\
26 & 3 & 13 & -2 \\
\end{array}
\]

\[
65 \cdot 3 + 91 \cdot (-2) = 195 - 182 = 13 \quad \text{check}
\]

\[
x = 3, \quad y = -2
\]
(10) 3. Prove by induction that for any positive integer \( n \),
\[ 1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2 \]

When \( n = 1 \), \( 1 = 1^2 \), so the statement is true.
Assume the statement is true for \( n \), \( 1 + 3 + 5 + \cdots + (2n - 1) = n^2 \).
Then
\[ 1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = n^2 + (2n + 1) = (n + 1)^2. \]
Thus the statement is true for \( n + 1 \). \( \text{QED} \).

(8) 4. Use properties of congruences to compute the following numbers modulo 7. (You can check your work on a calculator, but show how the properties are used here.)

(a) \( 707 \cdot 145 - 1403 \equiv 0 \cdot 145 - 3 \equiv -3 \equiv 4 \pmod{7} \)
\[ 707 \equiv 0 \pmod{7} \]
\[ 1403 \equiv 3 \pmod{7} \]

(b) \( 78^2 + 72^5 \equiv 1^2 + 2^5 \equiv 1 + 32 \equiv 33 \equiv 5 \pmod{7} \)
\[ 78 \equiv 1 \pmod{7} \]
\[ 72 \equiv 2 \pmod{7} \]

Check:
\[ 78 + 72 = 150 \equiv 3 \]
\[ 150 + 72 = 222 \equiv 5 \]

(5) 5. Find \( 2^{123} \pmod{15} \).

First note that \( 2^4 = 16 \equiv 1 \pmod{15} \)
\[ 2^{123} = (2^4)^{30} \cdot 2^3 \equiv 1^{30} \cdot 2^3 \equiv 8 \pmod{15} \]

Every positive integer \( n > 1 \) can be expressed uniquely as a product of primes.

7. Prove that there are infinitely many primes.

**Proof by contradiction:** Suppose there are only finitely many primes, say \( p_1, p_2, \ldots, p_k \). Let \( N = p_1 p_2 \cdots p_k + 1 \). Then \( n \) has a prime divisor \( p_i \) for some \( 1 \leq i \leq k \) (by FTA). Since \( p_i | n \) and \( p_i | p_1 p_2 \cdots p_k \) it follows that \( p_i | (n - p_1 p_2 \cdots p_k) \), that is, \( p_i | 1 \), a contradiction. Thus there are \( \infty \) many primes.

8. Solve the following congruences.

a) \( 7x \equiv 5 \pmod{13} \)  
   By inspection \( 7 \cdot 2 = 14 \equiv 1 \pmod{13} \)  
   \[ 2 \cdot 7x \equiv 2 \cdot 5 \pmod{13} \]  
   \[ x \equiv 10 \pmod{13} \]  
   \[ \{10\}_{13} \]  
   Either answer is okay.

b) \( 2x \equiv 4 \pmod{12} \)  
   \[ \gcd(2, 12) = 2 | 4 \]  
   \[ 2x = 4 + 12y \]  
   \[ x = 2 + 6y \]  
   \[ x \equiv 2 \pmod{6} \]  
   \[ \{2\}_6 \text{ or } \{2\}_{12} \text{ or } \{8\}_{12} \]  
   All 3 answers are correct.
9. Prove Euclid’s lemma: If \( a, b, c \) are integers with \( a \mid bc \) and \( \gcd(a,b) = 1 \), then \( a \mid c \).

Since \( \gcd(a,b) = 1 \), there exist integers \( x, y \) with \( ax + by = 1 \).

Then \( c = c(ax + by) = c(ax) + (bc)y \),
\[ \Rightarrow \quad c = a(cx) + (bc)y. \]

Since \( a \mid a \) and \( a \mid bc \) it follows that \( a \mid a(cx) + (bc)y \), that is, \( a \mid c \).

10. a) Find the continued fraction expansion of \( \sqrt{2} = 1.414213562\ldots \). (You can use your calculator if you like. Go down at least four levels and discover a pattern.)

\[ \sqrt{2} = 1 + \frac{1}{\sqrt{2} - 1} = 1 + \frac{1}{1 + \frac{1}{\sqrt{2} - 1}} = 1 + \frac{1}{2 + \frac{1}{\sqrt{2} - 1}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} - 1}}} \]

\[ = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} - 1}}}} \]

Note \( \frac{\sqrt{2} + 1}{\sqrt{2} - 1} = \frac{2 + \sqrt{2}}{2 - \sqrt{2}} = \frac{2 + \sqrt{2}}{2 - \sqrt{2}} \times \frac{2 + \sqrt{2}}{2 + \sqrt{2}} = \frac{2 + 2\sqrt{2} + 2}{4 - 2} = \frac{4 + 2\sqrt{2}}{2} = 2 + \sqrt{2} \)

= 2 + (\sqrt{2} - 1)

\[ \Rightarrow \text{pattern repeats} \]

b) Find the first five “best” rational approximations of \( \sqrt{2} \). (coming from the continued fraction expansion). Start with \( \frac{1}{1} \). Express your answers as reduced fractions.

\[
\begin{array}{cccccc}
0 & 1 & 1 & 2 & 2 & 2 \\
1 & 1 & 3 & 7 & 17 & 41 & 99 \\
& & 1 & 2 & 5 & 12 & 29 & 70 \\
\end{array}
\]

\[ \frac{1}{1} = 1 \]
\[ \frac{3}{2} = 1.5 \]
\[ \frac{7}{5} = 1.4 \]
\[ \frac{17}{12} = 1.416 \]
\[ \frac{41}{29} = 1.4137... \]

c) Explain why in Europe a standard note pad is of size 297 mm by 210 mm. (A piece of paper of size \( x \) by \( y \) with \( x > y \) is designed so that if it is folded in two lengthwise the resulting rectangle has the same proportions as the original rectangle, that is, \( \frac{x}{y} = \frac{y}{x/2} \).)

\[
\left( \frac{x}{y} \right)^2 = 2 \quad \Rightarrow \quad \frac{x}{y} = \sqrt{2}.
\]
Thus \( x, y \) are chosen so that \( \frac{x}{y} = \sqrt{2} \). This is a best rational approximation of \( \sqrt{2} \). Now \( \frac{297}{210} = \frac{99}{70} \) which is the sixth number in the list of best approximations (see part (b)).